In the Drawings

Applicants have enclosed an annotated version of previously presented FIG. 7 showing the amendments made to the figures, and have also enclosed a clean-copy replacement sheet that incorporates the changes noted in the red-lined figure. Applicants have also enclosed newly submitted drawings FIG. 7B and 7C, which add no new matter to this application.

REMARKS

This is a full and timely response to the outstanding non-final Office Action mailed January 3, 2006. Through this response, claims 1, 2, 6, 10, 21, 22, 24, 26, 32, 35, and 40 have been amended; and claims 5, 23, 25, 30, 31, 33, 34 and 39 have been canceled without prejudice, waiver, or disclaimer. Reconsideration and allowance of the application and pending claims are respectfully requested.

I. Allowable Subject Matter

Applicants appreciate the Examiner's indication that claims 10-17, 30, and 39-46 would be allowable if rewritten to include all of the limitations of the base claims and any intervening claims.

In that it is believed that every rejection has been overcome, it is respectfully submitted that every claim that remains in this application is presently in condition for allowance.

II. Drawings Objection

The drawings have been objected to under 37 C.F.R. 1.84(p)(4) because reference characters 700, 1100, and 1200 have all be used to designate the subprocessor.

In response to this objection, a clean copy of FIG. 7A, a replacement sheet for previously submitted FIG. 7, and a marked-up copy of previously submitted FIG. 7 that indicates all changes in red ink have been included with this Response. Also, new sheets containing FIGS. 7B and 7C have been enclosed. No new matter has been added.

In view of the above-noted amendments to the drawings, Applicants respectfully submit that the drawings are acceptable and respectfully request that the objection be withdrawn.

III. Specification Objection

The specification has been objected to for containing various informalities. Specifically, the Office Action identifies that the section Detailed Description of the Invention is titled Detailed Description of Drawings. On page 1, lines 23-24, it is stated that the proposal was submitted to "the National Institute of Standards (NIS)". The correct name of this organization is the National Institute of Standards and Technology (NIST).

In response to the objection, Applicants have amended the specification to incorporate these suggestions from the Examiner. Although these amendments effect various cosmetic changes to the specification, it is respectfully asserted that no new matter has been added. In view of these amendments, Applicants respectfully submit that the specification is not objectionable, and therefore respectfully request that the objection be withdrawn.

IV. Claim Rejections - 35 U.S.C. § 112, Second Paragraph

A. Statement of the Rejection

Claims 22 and 32 were rejected under 35 U.S.C. § 112, second paragraph, as allegedly indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention. In particular, the Examiner states that . . .

Claim 22 recites the limitation "the host memory" in line 2 of the claim. The Office Action alleged that there is insufficient antecedent basis for this limitation in the claim, as claim 22 is an independent claim and does not previously state a host memory.

Claim 32 recites the limitation "the host memory" in line 2 of the claim. The Office Action alleged that there is insufficient antecedent basis for this limitation in the claim, as claim 32 is an independent claim and does not previously state a host memory.

B. Discussion of the Rejection

In response to the rejections, Applicants have amended claims 22 and 32. In view of the amendments, it is respectfully asserted that claims 22 and 32 define the invention in the manner required by 35 U.S.C. § 112. Accordingly, Applicants respectfully request that the rejections to these claims be withdrawn.

V. Claim Rejections - 35 U.S.C. § 102(e)

A. Statement of the Rejection

Claims 1-4, 21-24, and 32-33 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by *Key et al.* ("*Key*," U.S. Pat. No. 6,173,386). Applicants respectfully traverse this rejection.

B. Discussion of the Rejection

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(e).

In the present case, not every feature of the claimed invention is represented in the *Key* reference. Applicants discuss the *Key* reference and Applicants' claims in the following.

1. Rejection of independent claim 1

Independent claim 1 recites:

> 1. A system for enciphering information, comprising:
> a first memory access unit configured to retrieve data from a host memory;
> a staggered FIFO unit ***configured as a hardware logic component*** to receive the retrieved data from the host memory, the staggered FIFO unit further configured to perform a ShiftRow step of an Advanced Encryption Standard (AES) algorithm on the data to produce row-shifted data;
> a second memory access unit configured to receive the produced row-shifted data and perform a byte substitution using the row-shifted data to produce byte-substituted data;
> logic configured to receive the byte-substituted data and expand the byte-substituted data to produce manipulated data using a designated expansion algorithm; and
> a subprocessor memory configured to receive and store the manipulated data.

(*Emphasis added*).

There is at least one fundamental distinction between the claimed embodiments and the cited *Key* reference. *Key* states that the parallel processing system disclosed therein may be used to implement data encryption standard (DES) algorithms, an encryption standard known in the art as an inferior predecessor to Advanced Encryption Standard (AES). However, parallelism is achieved, according to the reference, by "dividing the DES tables among the various dedicated memory resources." *Key*, column 15, lines 18-20. It would be appreciated that dividing DES tables among the various memory resources would not achieve performance and efficiency improvements similar to the claimed invention. The reference does not disclose a system capable of manipulating data consistent with the AES algorithm as the data is being loaded into processor memory. It would be appreciated that utilizing a system of the cited reference would likely require all of the data to be "apportioned" and then loaded into memory before data manipulation can occur because data

encryption can be performed in software in a system of the cited reference. *Key*, column 15, line 17.

Further, the reference does not disclose a second memory access unit that is also capable of performing a byte substitution to produce byte substituted data. The Office Action points to figure 3 of the cited reference but does not identify a reference numeral that the Examiner contends is corresponding to at least this element of the claimed invention. Also, the reference does not indicate or demonstrate to a person of ordinary skill in the art how the teachings disclosed in the reference can be used to implement a staggered FIFO unit configured as a hardware logic component to receive retrieved data from host memory, where the staggered FIFO unit is also configured to perform a ShiftRow step of the AES algorithm. The Office Action cites column 15, lines 9-21 of *Key* as disclosing information which anticipates this element of the claimed invention. However, this passage clearly states that "encryption functions are performed in software." *Key*, column 15, lines 9-21. In contrast, the claimed invention includes a staggered FIFO unit configured as a hardware logic component.

While *Key* discloses a plurality of "processing elements," which are separate CPU cores within a parallel processor, the reference does not disclose a system able to encipher information including a first memory access unit, a second memory access unit, a staggered FIFO unit configured as a hardware logic component that performs a ShiftRow step, logic to expand byte substituted data using a designated expansion algorithm and subprocessor memory. In other words, the cited reference does not disclose a system with the capability to manipulate data consistent with the AES algorithm ***as the data is being loaded into processor memory***. Again, the system of *Key* would likely require that the data first be loaded into processor memory before manipulation of the data consistent with the AES can occur.

For at least the above reasons, Applicants submit that independent claim 1 is allowable over the cited reference because it does not disclose, teach or suggest all elements of the claimed embodiments.

2. Rejection of claims 2-4

Applicants have amended claim 2 to advance prosecution and have incorporated allowable subject matter from previously presented dependent claim 5. Accordingly, Applicants submit that independent claim 2 is allowable because the cited reference does not disclose, teach or suggest all of the elements of the claimed invention. Claim 2 recites:

> 2. a host processor comprising a host memory, the host memory having data;
>
> a subprocessor having a subprocessor memory, ***the subprocessor configured to retrieve the data from the host memory and manipulate the data as the data is being loaded into the subprocessor memory***, the subprocessor further comprising a staggered FIFO unit configured as a ***hardware logic component*** to receive the retrieved data from the host memory, the staggered FIFO unit further configured to perform a ShiftRow step of the AES algorithm on the data to produce row-shifted data.

(*Emphasis added*).

As noted above in reference to independent claim 1, the cited *Key* reference does not disclose, teach or suggest a system capable of manipulating data consistent with the AES algorithm as the data is being loaded into the subprocessor memory. Further, column 15, lines 9-21 of *Key* state that "encryption functions are performed in software." In contrast, the claimed embodiments include a staggered FIFO unit configured as a hardware logic component that is also configured to perform a ShiftRow step of the AES algorithm. A "processing element" of the *Key* reference likely requires that data be completely loaded within each processing element before manipulation of the data consistent with the AES algorithm can occur, as encryption functions are performed in

software. *Id.* For at least the foregoing reasons as well as those noted above in reference to independent claim 1, Applicants submit that independent claim 2 is allowable over the cited *Key* reference.

Because independent claim 2 is allowable over *Key*, dependent claims 3 and 4 are also allowable as a matter of law for at least the reasons that the dependent claims 3 and 4 contain all elements of their respective base claim. See, *e.g.*, *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

3. Rejection of claims 22 and 24

The Office Action rejected claims 22 and 24 under 35 U.S.C. § 102(e) as allegedly anticipated by *Key*. The Office Action also noted that dependent claim 30 would be allowable if re-written in independent form including all the limitations of its base claim, independent claim 21. Accordingly, to advance prosecution, Applicants have incorporated the limitations of previously presented dependent claim 30 into independent claim 22 and respectfully submit that the claim is in condition for allowance. Similarly, Applicants submit that because claim 22 is allowable over *Key*, dependent claim 24 is allowable as a matter of law for at least the reason that the dependent claim 24 contains all elements of its base claim. See, *e.g.*, *In re Fine*, 837 F.2d 1071 (Fed. Cir. 1988).

4. Rejection of claim 21

With regard to independent claim 21, Applicants have incorporated limitations similar to independent claim 22, as noted above, and respectfully submit that independent claim 21 is also in condition for allowance for similar reasons.

5. Rejection of claim 32

The Office Action rejected independent claim 32 under 35 U.S.C. § 102(e) as allegedly anticipated by *Key*. The Office Action further notes that dependent claim 39 would be allowable if re-written in independent form containing all the limitations of the base and any intervening claims. To advance prosecution, Applicants have amended independent claim 32 accordingly, and respectfully request that the rejection of claim 32 be withdrawn.

Due to the shortcomings of the *Key* reference described in the foregoing, Applicants respectfully assert that *Key* does not anticipate Applicants' claims. Therefore, Applicants respectfully request that the rejection of these claims be withdrawn.

VI. Claim Rejections - 35 U.S.C. § 103(a)

A. Rejection of Claims

Claims 5-9, 18, 20, 25-29, 31, 34-38, 47, and 49 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Key* in view of *Daemen and Rijmen* ("*Daemen et al.*," "AES Proposal: Rijndael", 03/09/1999, pages 8 and 10). Claims 19 and 48 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Key* and *Daemen* in view of U.S. Patent No. 5,003,597 to Merkle (*Merkle*). Applicants respectfully traverse these rejections.

B. Discussion of the Rejection

Applicants submit that claims 6-9, 18-20 are allowable because they depend from allowable independent claim 2. For at least this reason Applicants submit that the rejection of independent claim 2 should be withdrawn. In addition, Applicants submit that claims 10-17, which also contain allowable subject matter as indicated by the Office Action are also in condition for allowance.

Applicants further submit that dependent claims 26-29 are allowable because they depend from allowable independent claim 22. Similarly, Applicants also submit that claims 35-38 and 40-49 are allowable because they depend from allowable independent claim 32.

VII. Canceled Claims

As identified above, claims 5, 23, 25, 30, 31, 33, 34 and 39 have been canceled from the application through this response without prejudice, waiver, or disclaimer. Applicants reserve the right to present these canceled claims, or variants thereof, in continuing applications to be filed subsequently.

CONCLUSION

Applicants respectfully submit that Applicants' pending claims are in condition for allowance. Favorable reconsideration and allowance of the present application and all pending claims are hereby courteously requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (770) 933-9500.

No fee is believed to be due in connection with this Amendment and Response to Office Actoin. If, however, any fee is deemed to be payable, you are hereby authorized to charge any such fee to deposit account 20-0778.

Respectfully submitted ,

THOMAS, KAYDEN, HORSTEMEYER & RISLEY, L.L.P.

By: _____
Daniel R. McClure, Reg. No. 38,962

100 Galleria Parkway
Suite 1750
Atlanta, Georgia 30339-5948
(770) 933-9500

Annotated Sheet

Title: A System and Method for Executing Advanced Encryption Standard (AES) Algorithm
Inventor(s): Yu, et al.; Page 8 of 59

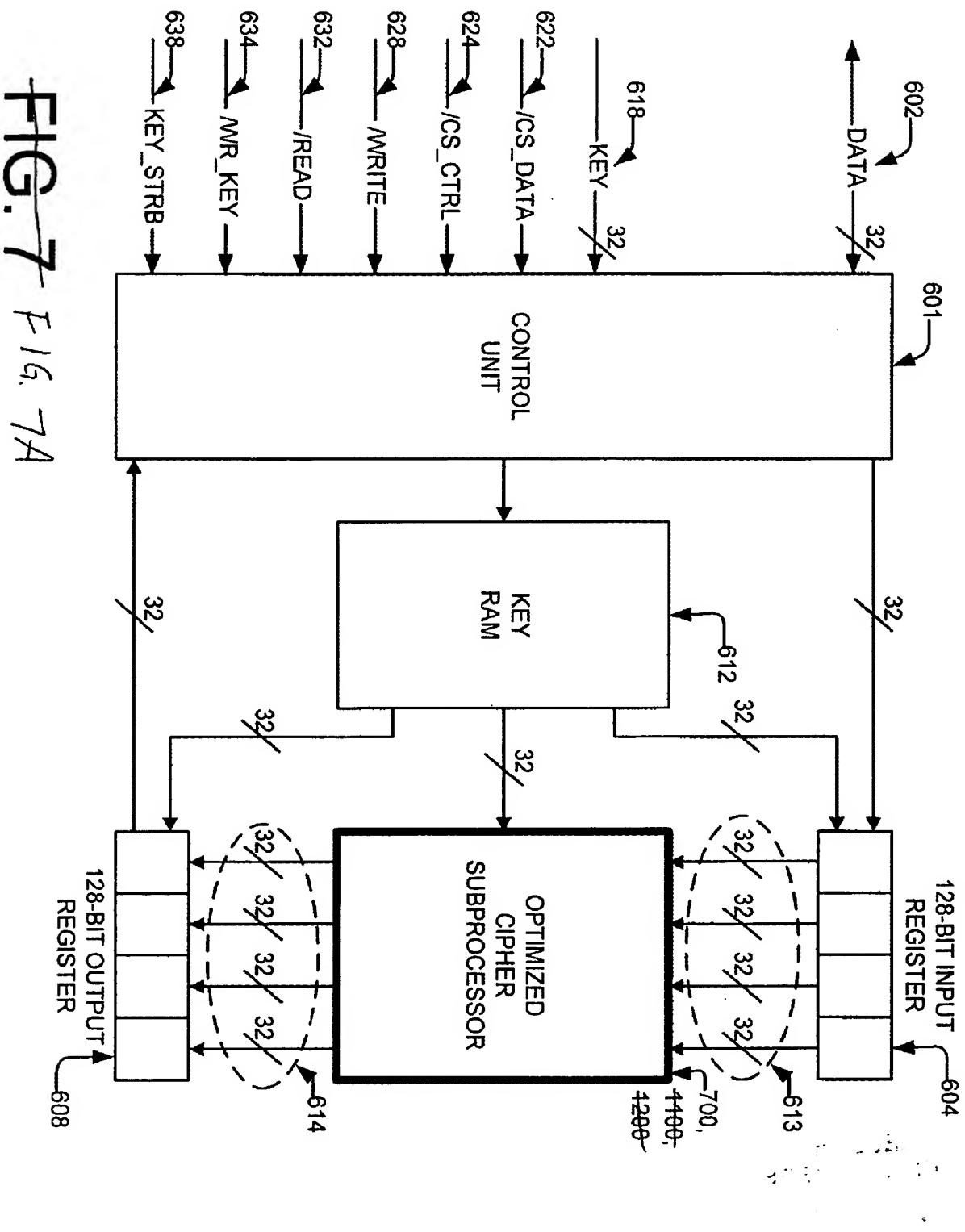

FIG. 7 FIG. 7A